ライフスタイル認証の活用事例とその検証：低リスクシナリオ

小林 良輔[1]　佐治 信之[2]　山口 利恵[1]

概要：インターネット技術の浸透やキャッシュレス化が進む昨今では，個人認証を求められるケースが増えてきている．従来の個人認証では ID ／パスワードや署名，また近年では生体情報などが求められる．しかしながら，従来の手法では認証時にユーザーに対して何らかの入力が求められ，ユーザーの負担が大きくなってきている．そこでユーザー利便性の観点から，一部のケースでは単純に端末所持や IC カード所持のみといった，簡易な手法で個人を認証する方法がとられている．一方でこのような簡易手法は，安全性はあまり考慮されていない．この課題に着目し，我々は簡易個人認証にライフログを利用することで，ユーザー利便性を損なわずに少し安全性を上げる手法を提案する．

キーワード：UWS，個人認証，ライフログ，ライフスタイル認証，スマートフォン

Use Case of Lifestyle Authentication and Its verification : Low Risk Scenario

Ryosuke Kobayashi[1]　Nobuyuki Saji[2]　Rie Shigetomi Yamaguchi[1]

Abstract: In recent years, as the penetration of Internet technology and cashless systems are advancing, people are required for user authentication in a number of cases. In conventional user authentication, ID / password, signature, biological information etc. are required. However, with these methods, some input from the user is required at the time of authentication, and the burden on the user is getting larger. Therefore, some cases just require simple user authentication such as holding the user's device or possessing the IC card from the viewpoint of user convenience. On the other hand, such simple methods are considered not to be much safety. Focusing on this issue, we propose a user authentication method utilizing life-log in order to raise the safety slightly without losing user convenience.

Keywords: UWS, User Authentication, Life-Log, Lifestyle Authentication, Smartphone

1. はじめに

近年，オンラインショッピングや Social Networking Service (SNS) など，インターネットを利用した様々なサービスが提供されている．これらのサービスを利用において，サービスプロバイダーは誰が利用しているかを確認するためにユーザーに対して個人認証を求めている．またインターネット上に限らず実店舗でもキャッシュレス化が進んでおり，クレジットカード等で支払い可能なケースが増えてきている．この支払いにおいてもクレジットカードの持ち主が正しいかを確認するため，ユーザーは個人認証を求められる．このように近年では個人認証を求められるケースが増えてきている．

しかしながら個人認証を求められることは，ユーザーにとって負担が大きくなってきている．現状よく利用されている個人認証手法には PIN や ID/パスワードなどがあるが，認証を必要とするケースが増えてきたため，ユーザーが入力する手間がかかったり，また登録した PIN やパス

[1] 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
[2] 株式会社インフォコーパス
INFOCORPUS Inc.

ワードを忘れてしまい，再登録するというケースが増えてきている．Yahoo! JAPAN によると，提供するサービスでは，パスワード忘れによるパスワード再設定が毎日約 15,000 件行われている [1] とのことである．

ユーザーが認証情報を入力する負担を軽減するために，リスクの低いケースでは簡易的な個人認証を求めるサービスも存在する．クレジットカードでの支払いにおいて PIN の入力もサインも必要としないケースや，いつも利用している端末でオンラインサービス利用においてパスワードを入力しないケースなどである．クレジットカードを所持していることや，いつもと同じ端末を利用しているといったことが簡易的な認証になっているのである．ここでリスクが低いとは，悪意のあるユーザーが本来のユーザーになりすましてサービスを利用しても，サービスプロバイダーや本来のユーザーの被害額が小さいことを意味する．

このような簡易的な個人認証手法はユーザーにとって利便性が高い一方で，容易になりすまされる可能性がある．例えばいつも利用している端末を他人に使用されたり，端末情報を偽造したりすることでなりすますことが可能となる．サービスプロバイダーは容易になりすまされる可能性があることを前提として低リスクケースでのみ簡易個人認証手法を採用しているが，なりすまされる可能性が低くなることでサービスプロバイダーのリスクは軽減し，またもう少しリスクの高いケースでも簡易個人認証手法が採用される可能性も出てくる．そこで本論文ではユーザーの利便性を変えることなく，なりすましや認証情報偽造の可能性を現状よりも低くする認証手法について検討する．

ユーザーに意識した認証情報の入力を求めない個人認証手法として，ライフスタイル認証が提案されている [2][3]．ライフスタイル認証とは人の生活パターンが繰り返されることから，個人的特徴を抜き出し，認証に利用する手法である．IoT 技術が発達してきている昨今では，周辺のセンサー等から人の行動情報が自動的に収集されており，その情報を活用することで，ユーザーは意識せずとも認証することが可能となる．一方で人の行動パターンは一定ではないため，行動情報を活用した認証手法では高い精度を得ることができない．スマートフォンが収集する Wi-Fi 情報を活用した既存研究 [4] では，認証精度が 93.2%との結果が出ている．そこで本論文ではスマートフォンによって収集される位置情報と Wi-Fi 情報を組み合わせ，特定の条件の下で高い精度を得ることができる認証手法について提案する．

1.1 論文の構成

本論文は以下の通りに構成されている．2 章ではライフスタイル認証に関する既存研究について紹介しする．特に Wi-Fi 情報を利用した手法について，既存研究と本研究との差異について述べる．3 章では本論文で提案する個人認証手法の利用シナリオについて説明する．4 章では本論文で提案する個人認証手法について説明する．5 章では本研究で行った実験及びその結果について説明する．6 章では実験結果についての考察を述べる．最後に 7 章では本論文における結論と，今後の課題について記述する．

2. 関連研究

本章では近年提案された，ライフスタイル認証に関する既存研究について紹介する．本論文で提案する Wi-Fi 情報を活用した個人認証に関する既存研究について紹介し，Wi-Fi 情報の特徴や認証手法の概要について説明する．また，Wi-Fi 情報以外の行動パターン情報を活用した認証手法に関する既存研究についてもいくつか紹介する．

2.1 Wi-Fi 情報を活用した認証手法

Wi-Fi 情報を利用した個人認証に関する既存研究に [5][6][7][8] などがある．[5] ではスマートフォンが取得する，スマートフォン端末周辺の無線 LAN アクセスポイントの履歴情報を活用した個人認証手法を提案している．履歴情報の具体的なものとしては，アクセスポイントの BSSID (Basic Service Set Identifier) と取得した時間を活用している．この手法では 30 日分のデータを利用して個人ごとのテンプレートを作成し，1 日 (24 時間) 分のデータを認証情報としてテンプレートと比較をしている．

また [6] では 1 時間分のデータを認証情報としてテンプレートと比較している．1 時間での認証は 24 時間での認証と比べると精度が悪くなる結果となっている．ただし 1 時間での認証は昼間と夜間で精度に大きな差があり，ユーザーによっては夜間では 100% 認証に成功しているケースもある．

[8] でも 1 時間分のデータを認証情報とした実験を行っているが，[6] と比べて実験被験者数が増加している．[6] では実験被験者を 17 人で実施しているが，[8] では 47 人で実験を行っている．被験者数が増えても精度はほとんど変わっておらず，Wi-Fi 情報を利用した個人認証手法の有用であることを述べている．

無線 LAN アクセスポイントの履歴情報以外に，電波強度も活用した認証手法が [7] で提案されている．電波強度を活用することで，仕事や研究で普段同じ部屋にいる人同士でも認証精度を上げることができるとしている．また 1 時間の認証は 24 時間の認証と比べて精度が悪くなるが，[7] では平日・休日のパラメータを追加することで，条件によっては 1 時間での認証も可能であると述べている．

2.2 Wi-Fi 情報の特徴

ライフスタイル認証は人間の生活における行動パターンを活用した認証手法である．Wi-Fi 情報を活用した認証手法もライフスタイル認証の一要素として考えられ，同様に

行動パターンを活用している．この人間の生活における行動パターンは日々似てはいるが，まったく同じというわけではない．人間の行動にはゆらぎが存在するのである．

スマートフォンが取得する Wi-Fi の情報には，人間の行動のゆらぎが二つの面で表現される．一つ目は Wi-Fi 情報を取得する時間のゆらぎである．人は毎日同じような行動をしていても，時間がずれるということがある．この時間のずれは Wi-Fi 情報を取得する時間に表れることとなる．

二つ目は同じ Wi-Fi 情報を取得する頻度のゆらぎである．人の行動にはよく行うものもあれば，たまにしか行わない行動もある．よく行う行動時に取得する Wi-Fi 情報は取得頻度が高く，たまにしか行わない行動は取得頻度が低いというように，行動のゆらぎは Wi-Fi 情報の取得頻度に表れることとなる．

このように人間の行動にはゆらぎが存在するため，行動パターンを活用する個人認証手法はこのゆらぎを吸収するものでなければならない．特に Wi-Fi 情報を利用した個人認証手法においては，時間のゆらぎと取得頻度のゆらぎを吸収する必要がある．

2.3 Wi-Fi 認証手法概要

Wi-Fi 情報を利用した個人認証手法には登録モードと検証モードの二つのモードからなる．二つのモードの流れとしては，登録モードではテンプレートが作成され，検証モードでは入力された認証情報とテンプレートの比較が行われ，認証の合否を判定する，といったものである．

登録モードで作成されるテンプレートは 30 日間のデータを元に作成される．2.2 節で述べたように，Wi-Fi 情報を利用した個人認証手法は時間のゆらぎと取得頻度のゆらぎを吸収する必要があり，そのためにテンプレートは 30 日間のデータからゆらぎ吸収のための処理が施されて作成される．時間のゆらぎ吸収のためには時間丸めの処理が行われ，取得頻度のゆらぎ吸収のためにはアドレス選定・濃淡付与処理が行われる．ゆらぎ吸収のための処理が行われた後，認証情報との比較を行うために，二値化処理が行われる．

検証モードではテンプレートと比較するための認証情報が作成される．認証情報は [5] では 24 時間のデータを元に作成することが提案されているが，[6] などでは 1 時間のデータから作成することも提案されている．既存研究の実験結果では 24 時間のデータを元に作成した認証情報がより高い精度を出しており，本論文での実験では 24 時間のデータを元に認証情報を作成する．このように作成された認証情報をテンプレートと比較し，一致率を算出する．一致率があらかじめ定められたセキュリティパラメータ k より大きい場合には認証成功と判断する．

2.4 Wi-Fi 以外の情報を活用した認証手法

Tang ら [9] はデータマイニング手法を活用した，スマートフォンにおける個人認証手法を提案した．彼らはアプリケーション利用履歴と GPS のデータを収集し，このデータを使って実験を行った．実験結果から，これらのデータはユーザーの習慣をよく反映したものであると Tang らは述べている．しかしながら実験の被験者数は 10 人と規模が小さく，また認証精度も 70%程度とそれほど大きな結果ではなかった．

人の行動パターンを活用した個人認証手法の精度は，一般的に生体認証よりも小さくなる．認証精度を上げるためには複数の認証要素を組み合わせることが必要となってくるが，Fridman ら [10] はキーボード入力，アプリ利用履歴，閲覧サイト，端末位置の 4 つの要素を組み合わせて実験を行った．彼らはこれら 4 種類のデータを，被験者 200 人から，被験者自身の Android 端末を利用して 30 日間収集した．彼らの実験結果は EER (Equal Error Rate) が 0.01 となり，非常に精度の高いものとなった．

スマートフォン以外でもウェアラブル端末で収集されるデータを活用した既存研究もある．鈴木ら [11] はウェアラブル端末で収集された活動情報を利用し，cost-effective ユーザーモデルを提案し，個人認証に適用した．彼らは提案手法は，活動情報に含まれる人間の 1 日ごとの特徴と 1 時間ごとの特徴を活用したものである．実験は 70 人の被験者を対象に行われ，認証精度は 89.28%であった．

スマートフォンやウェアラブル端末などに搭載されているセンサーで収集された情報以外を個人認証手法に活用した既存研究もある．Sultana ら [12] は，社会における活動には個人ごとの独特の行動パターンが含まれていると主張しており，241 人の Twitter に投稿された内容を分析した．分析結果から，Twitter への投稿が頻繁であろうとなかろうと，この情報はユーザーごとに一意性，安定性，認識精度などの特性を有すると結論付けた．

3. 想定シナリオ

本章では，本論文で提案する個人認証手法が利用されるシナリオについて定義する．

3.1 ユースケース

近年、我々はスマートフォン端末で様々なアプリケーションを利用することができる．アプリケーションの中には利用するために個人認証を必要とするものもある．これらの中には SNS アプリのように一度認証情報を入力してログインすると次回からアプリ起動時に自動的にログインされるアプリや，銀行アプリのように起動のたびに認証情報の入力を求めるアプリなどがある．本論文での個人認証利用想定ケースは，一度認証情報を入力してログインすると次回からアプリ起動時に自動的にログインされるタイプ

のアプリを，スマートフォンで利用することとする．なお，以降は単純にユーザーを U，スマートフォン端末を D，アプリケーションを A，サービスプロバイダーを SP と表記する．

3.2 シナリオモデル

本節では 3.1 節で定義したユースケースにおいて，本論文で想定するシナリオのモデルについて説明する．まずは 2 つのタイプの認証情報について以下の通り定義する．

- 主要認証情報（MA）: U が意識して入力する認証情報．パスワードや生体情報などがあたる．
- 副次認証情報（SA）: ユーザーが意識せずに入力される認証情報．端末情報や IP アドレスなどがあたる．

本論文では主要認証情報は 1 つの要素のみからなり，副次認証情報は複数の要素から構成されると仮定する．主要認証情報は単に MA と表記し，副次認証情報は構成する要素 a_n を用いて，$SA(a_1, \cdots, a_n)$ と表記する．この 2 タイプの認証情報を SP がチェックすることにより，本論文における個人認証手法が利用されるケースの想定シナリオを以下の通りとする．なお，このチェック処理 C は認証情報を引数として U に紐づく ID を返却する関数として，以下の通り定義する．

$$C(MAorSA) = \begin{cases} U_{id} & (MAorSA \text{ が } SP \text{ に登録済}) \\ None & (MAorSA \text{ が } SP \text{ に未登録}) \end{cases}$$

(1) アプリ起動
U は D で A を起動する．この際に D に紐づく副次認証情報 $SA(a_1, \cdots, a_n)$ が自動的に SP に送信される．

(2) 副次認証情報チェック
SP は送信された副次認証情報を要素ごとにチェックする．$C(SA(a_i))$ $(i = 1 \sim n)$ がすべて同じ場合は (7) へ進む．

(3) 主要認証情報要求
SP は U に主要認証情報の入力を要求する．

(4) 主要認証情報入力
U は A に主要認証情報を入力し，SP に送信する．その際に自動的に副次認証情報 $SA(a_1, \cdots, a_n)$ が SP に送信される．

(5) 主要認証情報チェック
SP は送信された主要認証情報を要素ごとにチェックする．$C(MA) = None$ の場合は (3) に戻る．

(6) 副次認証情報登録
SP は送信された副次認証情報を，$C(SA(a_i)) = C(MA)$ $(i = 1 \sim n)$ となるように登録する．

(7) ログイン
A にログインする．

4. 提案手法

本研究の目的は，3 章において定義した，副次認証情報 $SA(a_1, \cdots, a_n)$ 構成する要素を増やすことによって，副次認証情報のみの簡易的な個人認証が，現状よりも高いリスクのケースで利用できるようにすることである．追加する要素はスマートフォン端末が収集する Wi-Fi 情報であるが，2 章で記述したように Wi-Fi のみを活用した既存の認証手法は，認証精度がそれほど高くない．副次認証情報による簡易個人認証が失敗すると，主要認証情報による認証に移るため，認証精度の低い要素は簡易認証の要素として適切ではない．そこで，Wi-Fi 情報だけではなく，位置情報と組み合わせた新しい簡易個人認証手法を本論文では提案する．なお既存の簡易個人認証手法と同様，本論文で提案する手法は端末を他人が利用した際のなりすましについては考慮しない．

4.1 概要

本論文で提案するスマートフォン端末が収集する Wi-Fi 情報を活用した個人認証手法は，既存手法 [4] と同様，あらかじめ登録されるテンプレートと認証情報を比較することで行う．しかしながら，人の行動はいつも同じということはなくゆらぎが存在し，そのため同じテンプレートを認証に使用していることが認証精度を下げる要因になると考えられる．そこで本論文では，スマートフォン端末が収集する Wi-Fi 情報と位置情報には相関があることから，ユーザーがいる位置ごとにテンプレートを作成する手法を提案する．

4.2 メッシュコード

本論文では位置を表す情報としてメッシュコード [13] を使用する．ここでメッシュとは，緯度・経度に基づいて地域をほぼ同じ大きさの網目に分けたものであり，メッシュを識別するためのコードをメッシュコードと呼ぶ．メッシュはその大きさによりいくつかの種類に分けられ，それぞれに対して区分方法が定まっている（表 1）．

4.3 テンプレート

本論文で提案する個人認証手法に使われるテンプレートは，上で述べたようにユーザーがいる位置ごとに作成される．そこでまずは，テンプレート作成におけるユーザーがいる位置ごと，という意味について説明する．テンプレート登録期間のうち，1 番長い時間いた位置 (l_1)，2 番目に長い時間いた位置 (l_2)，3 番目 (l_3)，4 番目 (l_4)，その他の位置 (l_5) と 5 つに分割し，この 5 つの位置それぞれについてテンプレートを作成する．ユーザーが長い時間いる位置とは，そのユーザーの特徴を表した情報であると考えられ，

表 1　メッシュの区分方法

メッシュの種類	区分方法	緯度の間隔	経度の間隔	一片の長さ
第 1 次メッシュ	全国の地域を偶数緯度及びその間隔（120 分）を 3 等分した緯度における緯線並びに 1 度ごとの経線とによって分割してできる区域	40 分	1 度	約 80km
第 2 次メッシュ	第 1 次メッシュを緯線方向及び経線方向に 8 等分してできる区域	5 分	7 分 30 秒	約 10km
第 3 次メッシュ	第 2 次メッシュを緯線方向及び経線方向に 10 等分してできる区域	30 秒	45 秒	約 1km
2 分の 1 地域メッシュ	第 3 次メッシュを緯線方向，経線方向に 2 等分してできる区域	15 秒	22.5 秒	約 500m
4 分の 1 地域メッシュ	2 分の 1 地域メッシュを緯線方向，経線方向に 2 等分してできる区域	7.5 秒	11.25 秒	約 250m
8 分の 1 地域メッシュ	4 分の 1 地域メッシュを緯線方向，経線方向に 2 等分してできる区域	3.75 秒	5.625 秒	約 125m
16 分の 1 地域メッシュ	8 分の 1 地域メッシュを緯線方向，経線方向に 2 等分してできる区域	1.875 秒	2.8125 秒	約 62.5m

その位置ごとにテンプレートを作成することで，よりユーザーを特徴づけるテンプレートが作成されると考えられる．

テンプレート作成時の位置を表す情報としては第 3 次メッシュを利用する．第 1 次メッシュのように広いメッシュを採用すると，行動範囲が常に同じメッシュ内になる可能性が高くなり，また 16 分の 1 地域メッシュのように狭いメッシュだと，1 番目から 4 番目の位置すべてが，例えば自宅周辺など近接したメッシュとなる可能性が高くなる．このような現状ではユーザーを特徴づける位置ごとにテンプレートを作成できないと考えられるため，第 3 次メッシュを利用する．

第 3 次メッシュでテンプレート登録期間にいた位置を 5 分割し，それぞれの場所についてテンプレートを作成する．本研究でのテンプレートは，テンプレート登録期間のうち最も長い期間キャッチした，5 つの BSSID のリストとする．すなわち，ユーザー U における場所 l_i $(i = 1 \sim 5)$ のテンプレートを $T_{l_i}(U)$ とし，テンプレート登録期間内に場所 l_i で最も長い時間キャッチした BSSID5 つを $b_1, b_2, \cdots, b_5$ としたとき，

$$T_{l_i}(U) = \{b_1, b_2, \cdots, b_5\}$$

と表記する．

4.4　チェック処理

本節では認証情報と前節で説明したテンプレートを比較し，認証情報はユーザー本人の情報かどうかをチェックする処理について説明する．認証情報は認証時にスマートフォンが収集するデータで，スマートフォン端末の位置情報 (l) と端末周辺の Wi-Fi 情報 $(b_{i_1}, b_{i_2}, \cdots)$ から構成されている．このとき，認証情報 $SA = \{l, b_{i_1}, b_{i_2}, \cdots\}$ とテンプレート $T_{l_i}(U) = \{b_1, b_2, \cdots, b_5\}$ のチェック処理 $C(SA)$ を以下の通り定義する．

$l = l_i$ のとき，

$$C(SA) = \begin{cases} U_{id} & (|\{b_{i_1}, b_{i_2}, \cdots\} \cap \{b_1, b_2, \cdots, b_5\}| \geq 1) \\ None & (|\{b_{i_1}, b_{i_2}, \cdots\} \cap \{b_1, b_2, \cdots, b_5\}| = 0) \end{cases}$$

これは 3 節で定義したチェック処理の，認証情報がサービスプロバイダーに登録されているかどうかの条件を明確にしたものである．

5.　実験

本章では本研究における実験で利用したデータセット，4 章で説明した手法の実装，および実験結果について記述する．

5.1　データセット

本実験では，東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター次世代個人認証技術講座が 2017 年 1 月〜4 月に実施した，MITHRA プロジェクト [14] で収集したデータを用いた．

5.1.1　データ収集仕様

MITHRA プロジェクトに参加した 57,046 人のうち，MITHRA アプリをインストールした 16,027 人から本研究の対象データである位置情報と Wi-Fi 情報を収集した．本実験では Android 版の MITHRA アプリをインストールしたユーザーを対象にし，Android 版 MITHRA アプリは 5 分ごとにデータを収集し，1 日に一度サーバへ収集したデータをアップロードする．収集した本研究に関するデータは，スマートフォン端末周辺の Wi-Fi ルータの BSSID，端末の位置情報，および受信した日時である．

5.1.2　データ選定

Android 版 MITHRA アプリで収集されたデータから以下の方法で実験に利用するデータを選定した．

- Android 版 MITHRA アプリをインストールした 1,391 人のうち 60 日以上実験に参加した中からランダムで 100 人を選出し，本研究の実験対象ユーザーとした．

- 対象日実験対象としたユーザー 100 人は，MITHRA プロジェクト参加期間がそれぞれ異なるため，それぞれの参加期間のうち最初の 60 日に収集されたデータを本実験での利用対象とした．

5.2 実装

5.2.1 実験期間

本実験では 60 日間のデータを利用して実験を行った．実験期間 60 日間のうち，最初の 30 日をテンプレート登録期間とし，残りの 30 日間をテスト期間として，テスト期間のデータから認証情報を作成しテンプレートとのチェックを行った．

5.2.2 評価方法

MITHRA アプリが 5 分に 1 度収集するデータを認証情報とし，テスト期間のデータ数だけテンプレートとの比較を行った．比較を行った回数のうち，結果 U_{id} が返却されたものの割合を認証精度とした．認証精度の結果は位置ごとに算出した．また，認証精度の結果を算出する際の位置情報は，第 3 次メッシュから 16 分の 1 地域メッシュの 5 つの区分方法において算出した．Wi-Fi 電波の届く距離はせいぜい 100m 程度であり，広いメッシュだと位置情報と Wi-Fi 情報の相関が弱まってしまうと考えられる．そのため，メッシュの大きさを変えながら認証精度の評価を行った．

5.3 実験結果

図 1 は位置ごとおよび区分ごとの実験結果でユーザー 100 人の平均値を表したグラフであり，表 2 はその結果を数値で表したものである．なお，テンプレートの位置は第 3 次メッシュを使用しているため，結果の 2 分の 1 地域メッシュ以降はテンプレートの位置とマッチするメッシュが複数存在する．結果に表した値は複数のメッシュのうち，値が最大となったものである．

表 2 位置ごとおよび区分ごとの認証精度

認証精度	l_1	l_2	l_3	l_4	l_5
第 3 次メッシュ	0.930	0.731	0.429	0.442	0.100
2 分の 1 地域メッシュ	0.939	0.771	0.454	0.466	0.100
4 分の 1 地域メッシュ	0.945	0.789	0.479	0.477	0.100
8 分の 1 地域メッシュ	0.946	0.803	0.476	0.479	0.100
16 分の 1 地域メッシュ	0.947	0.812	0.454	0.472	0.100

実験結果から，テンプレート登録期間によくいた位置ほど認証精度が高く，またメッシュの区分が狭いほど認証精度が高くなっていることがわかる．

また表 3 はテスト期間中に，$l_1 \sim l_5$ にいた時間の割合を表したもので，こちらもユーザー 100 人の平均値である．認証精度と同様，2 分の 1 地域メッシュ以降は認証精度が

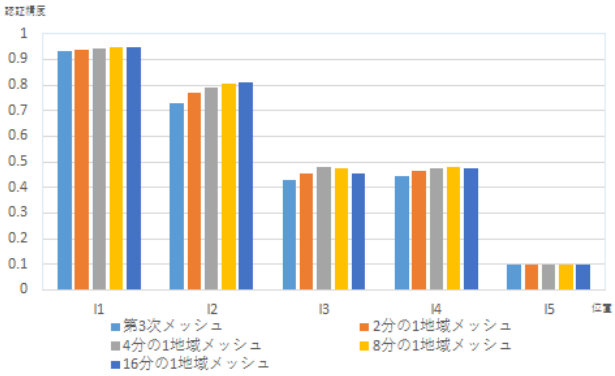

図 1 位置ごとおよび区分ごとの認証精度

最大となるメッシュの結果を表示している．表 2 と表 3 から，位置情報を第 3 次メッシュの区分で考えた時は 0.695 の割合で 0.930 の認証精度を得ることができ，16 分の 1 地域メッシュの区分で考えた時は 0.604 の割合で 0.947 の認証精度を得ることができることがわかる．

表 3 位置ごとおよび区分ごとの滞在時間割合

滞在時間割合	l_1	l_2	l_3	l_4	l_5
第 3 次メッシュ	0.695	0.145	0.025	0.013	0.123
2 分の 1 地域メッシュ	0.677	0.133	0.021	0.011	0.123
4 分の 1 地域メッシュ	0.661	0.127	0.018	0.009	0.123
8 分の 1 地域メッシュ	0.630	0.119	0.017	0.008	0.123
16 分の 1 地域メッシュ	0.604	0.110	0.014	0.007	0.123

図 2 は 16 分の 1 地域メッシュで場所 l_1 の場合のユーザーごとの認証精度である．この図から認証精度が最も低いユーザーで 0.6 程度の精度を得ており，大部分のユーザーは 0.9 以上の精度を得ていることがわかる．図 3 は図 2 で認証精度が 0.9 以上となったユーザー数をヒストグラムで表している．この図からはさらに，大部分のユーザーが 0.99 以上の精度を得ていることがわかり，100 人中 7 人は認証精度が 1 となっている．表 2 からは認証精度の平均値は 0.947 程度の結果となったが，図 23 から多数のユーザーは精度 0.99 以上と高い結果を得ることができたことがわかる．

6. 考察

本章では 5.3 節での実験結果から，提案手法の有用性について考察を行う．

6.1 提案手法の有用性

図 1 から本論文で提案した手法は，常に簡易な個人認証として利用できる手法とは言えないことがわかった．しかしながら，場所 l_1 にいるときは高い認証精度を得ることができ，個人認証に利用できる可能性はある．そのため場所

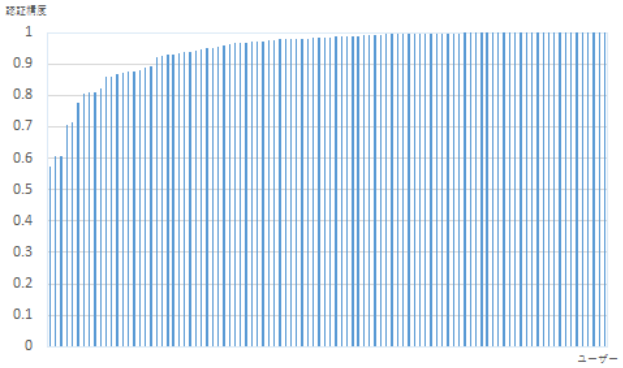

図 2 16 分の 1 地域メッシュで場所 l_1 の場合のユーザーごとの認証精度

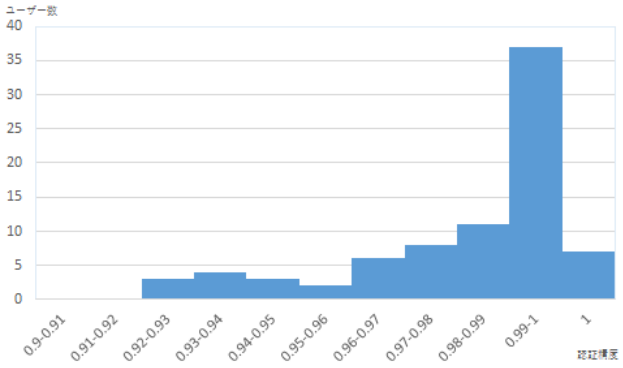

図 3 16 分の 1 地域メッシュで場所 l_1 の場合の認証精度ヒストグラム

l_1 にいる時は，3.2 節で記載した副次認証情報の認証要素として Wi-Fi 情報を追加し，l_1 以外にいる時は Wi-Fi 情報は認証要素としない，という利用の仕方が考えられる．実際に表 3 から 6 割程度の時間は場所 l_1 にいるということがわかり，場所 l_1 にいる時のみという条件を付けても，有用な手法であると考えられる．

6.2 精度の低いユーザー

図 23 から大部分のユーザーは表記の条件の下で高い認証精度を得ることができる一方で，一部のユーザーは低い認証精度となっていることがわかる．ユーザー 100 人のうち，19 人が認証精度 0.9 以下となっており，本節ではこの 19 人のユーザーについて考察を行う．メッシュは 16 分の 1 地域メッシュに限る．

図 4 は 19 人のユーザーごとに，場所 l_1 と l_2 それぞれにおいて認証精度を表したグラフである．表 2 を見ると，l_1 と l_2 の認証精度は l_1 の方が高いことがわかるが，対象としたユーザー 19 人に限ってみると，全体的に l_2 の方が精度が高いことが見て取れる．実に 19 人のうち，16 人が l_2 の方が精度が高い結果となった．（なお，2 人のユーザーはテスト期間中に l_2 で Wi-Fi 情報を取得していない．）

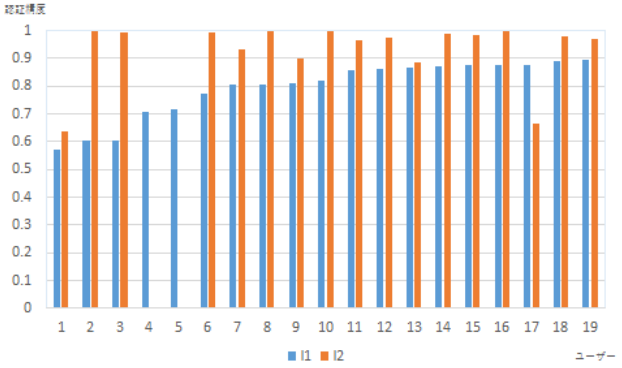

図 4 場所 l_1 と l_2 におけるユーザーごとの認証精度

表 4 対象ユーザー 19 人の場所 l_1 と l_2 における認証精度の平均値

	l_1	l_2
認証精度	0.795	0.934

長い時間滞在する場所はそのユーザーを特徴づける情報と仮定しており，表 2 などから一般的にはその仮定が正しいと考えられるが，図 4 の結果から，これらのユーザーに対しては l_1 より l_2 の方がユーザーを特徴づける情報である可能性がある．ユーザーによって，どういった情報がそのユーザーを特徴づける量となるのか判定できれば，さらに認証精度を高めることができると考えられる．

7. おわりに

本論文では，ユーザーの利便性を上げるために低リスクなケースにおいては簡易的な個人認証手法が実際に利用されていることを指摘し，現状よりも高いリスクがあるケースでも簡易的な手法が利用できるよう，認証要素を追加することを提案した．ユーザー利便性を下げないために，追加する認証要素はユーザーが意識的に入力する必要のない情報である必要があり，近年提案された Wi-Fi の情報を活用することを提案した．また，Wi-Fi 情報だけでは精度が十分に高くならない可能性があるため，位置情報と組み合わせる手法を提案した．その結果，特定の条件の下で多くのユーザーにとって高い認証精度を得ることができた．

6.2 節で考察した通り，一部のユーザーにとっては自身を特徴づける量が一般的なものと異なる可能性がある．ユーザーによってどういった情報がそのユーザーを特徴づける量となるのか判定できれば，さらに認証精度を高めることができると考えられ，判定する手法を見出すのは今後の課題となる．

参考文献

[1] マイナビニュース：Yahoo! JAPAN、パスワード入力が不要のログイン方法を導入，入手先 ⟨http://news.mynavi.jp/news/2017/04/20/220/⟩（参照 2017-08-24).

[2] 小林 良輔，疋田 敏朗，鈴木 宏哉，山口 利恵：行動センシングログを元にしたライフスタイル認証の提案，コンピュータセキュリティシンポジウム 2016 論文集，2016(2)，pp.1284-1290 (2016).

[3] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi: *Lifestyle Authentication*, Information Theory and Its Applications (ISITA), 2016 International Symposium on. IEEE, 2016 (Poster).

[4] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi: *Behavioral Authentication Method Utilizing Wi-Fi History Information Captured by IoT Device*, International Workshop on Secure Internet of Things (SIoT), 2017 International Workshop on. IEEE, (to appear).

[5] RYOSUKE KOBAYASHI and RIE Shigetomi YAMAGUCHI: *A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User*, Computing and Networking (CANDAR), 2015 Third International Symposium on. IEEE, 2015.

[6] 小林良輔，山口利恵： Wi-Fi 履歴情報を活用した複合認証における個人認証手法，コンピュータセキュリティシンポジウム 2015 論文集 2015.3 (2015): pp.889-896.

[7] 平岩啓，満保雅浩： 無線 LAN 情報の認証への応用の検討，電子情報通信学会論文誌 D 99.10 (2016): 1034-1044.

[8] RYOSUKE KOBAYASHI and RIE Shigetomi YAMAGUCHI: *One hour term authentication for Wi-Fi information captured by smartphone sensors*, Information Theory and Its Applications (ISITA), 2016 International Symposium on. IEEE, 2016.

[9] Yujin Tang, Nakazato Hidenori, and Yoshiyori Urano: *User authentication on smart phones using a data mining method*, Information Society (i-Society), 2010 International Conference on. IEEE, 2010.

[10] Lex Fridman, Steven Weber, Rachel Greenstadt and Moshe Kam: *Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location*, IEEE Systems Journal, 2016.

[11] Susuki Hiroya and Rie Shigetomi Yamaguchi: *Cost-Effective Modeling for Authentication and Its Application to Activity Tracker*, International Workshop on Information Security Applications. Springer, Cham, 2015.

[12] Madeena Sultana, Padma Polash Paul and Marina L. Gavrilova: *User Recognition From Social Behavior in Computer-Mediated Social Context*, IEEE Transactions on Human-Machine Systems 47.3 (2017): 356-367.

[13] 総務省：地域メッシュ統計の特質・変革，入手先 ⟨http://www.stat.go.jp/data/mesh/pdf/gaiyo1.pdf⟩（参照 2017-08-28).

[14] 鈴木 宏哉，小林 良輔，佐治 信之，山口 利恵：ライフスタイル認証実証実験レポート -MITHRA データセット-，マルチメディア，分散，協調とモバイル (DICOMO2017) シンポジウム，pp.223-230 (2017).